Lampi di Cassandra/ SPID2, l'opinione del NIST

(377)—Negli USA l'autenticazione a due fattori a mezzo SMS viene bocciata e sparirà presto dalla circolazione. E non è solo questione di…

Lampi di Cassandra/ SPID2, l'opinione del NIST

(377) Negli USA l'autenticazione a due fattori a mezzo SMS viene bocciata e sparirà presto dalla circolazione. E non è solo questione di malware

SPID2 è già stato oggetto di esternazioni di Cassandra: la nostra amica sosteneva che l'attuale offerta di SPID, limitata alla SPID2 con SMS, era insicura e controproducente ai fini della sicurezza, particolarmente per la possibilità di infezioni dello smartphone da parte di malware avanzati.

Agenda Digitale, quotidiano telematico di informazione, pubblicava un articolo nel quale, in buona sostanza, si sosteneva che se un device è infetto, e un attacco Man-in-the-browser o Man-in-the-middle è in corso, non c'è doppio fattore che tenga.

Anche se è senz'altro vero che non avere malware sul proprio smartphone sia cosa buona e giusta, nel contesto SPID si tratta di un'affermazione semplicistica, fuorviante e tecnicamente sbagliata, perché non tratta il nocciolo del problema.

In queste ore, il NIST (National Institute of Standards and Technology), ente statunitense che cura le standardizzazioni tecnologiche e che non è proprio l'ultimo arrivato nel settore, ha pubblicato il final draft del documento "Digital Authentication Guideline—Authentication and Lifecycle Management". La parte B del documento (Cassandra si scusa della pedanteria) pianta gli ultimi chiodi sulla bara della autenticazione a due fattori con SMS (2FA-SMS). Un sintetico riassunto della questione si trova su Slashdot.Ma citiamo direttamente la raccomandazione contenuta in questa imminente normativa. Il NIST raccomanda che le applicazioni utilizzino token fisici e crittografici. Il documento prevede, quasi a "malincuore", che essi possano attualmente assumere anche la forma di app per cellulari, quindi di dispositivi che possono essere rubati o "temporaneamente presi in prestito".

NIST sottolinea poi il fatto che la 2FA-SMS ha un altro punto debole che ha eroso la sua affidabilità, quello dei servizi VoIP: "Se la verifica fuori banda deve essere effettuata tramite un messaggio SMS su una rete pubblica di telefonia mobile, il gestore del processo deve assolutamente controllare che il numero di telefono pre-registrato in uso sia veramente associato con una rete mobile e non con un VoIP (o altro sistema telefonico basato su software)". Aggiunge inoltre che "la modifica del numero di telefono pre-registrato non deve essere possibile senza una *vera autenticazione a due fattori*, da utilizzare al momento del cambio numero. Il cambio del numero tramite SMS è deprecato, e non sarà più consentito nelle versioni future di questa guida."

In buona sostanza, oltre ai problemi legati ai malware avanzati che possono infettare uno smartphone (e certamente lo faranno) rendendo l'autenticazione a due fattori via SMS insicura, NIST individua altri due vettori di attacco: le reti VoIP e le problematiche legate al cambio del numero telefonico su cui ricevere l'SMS, che impediscono di usare la 2FA-SMS come metodo di autenticazione sicuro.Ricordiamo la definizione di base della 2FA: "Qualcosa che sai, più qualcosa che hai".Gli smartphone e le reti GSM non sono sotto il controllo dell'utente ma di terzi, legittimamente o illegittimamente, quindi non rappresentano un "qualcosa che hai". E

questa è un'ulteriore conferma che la SPID2, realizzata con SMS e non con token hardware, non dovrebbe proprio esistere.

Ma in Italia ci vorrebbe una catastrofe affinché la convenienza della 2FA-SMS, scelta per facilitare il "decollo" del PIN di Renzi della SPID, venisse messa in discussione.

Originally published at punto-informatico.it.

By Marco A. L. Calamari on February 8, 2022.

Canonical link

Exported from Medium on August 27, 2025.